

IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A data transmitting apparatus comprising:

a processor configured to generate first authentication data based on shared data shared with a data receiving apparatus;

a communication interface ~~command transmission unit~~ configured to transmit a first response request command to [[a]] said data receiving apparatus, said first response request command including said first authentication data, and ~~;~~ ~~a control unit configured to receive a first response message to the first response request command from the data receiving apparatus, the response message including second authentication data, which is generated~~ ~~[[in]] by the data receiving apparatus prior to the data receiving apparatus receiving the response request command, the authentication data being based on the shared data and shared with said data receiving apparatus; an expected value generation unit configured to generate an expected authentication value based on the shared data and a first sequence number, the sequence number included in the first response request command indicating a an ordinal position of the first response request command in a sequence of response request commands to be transmitted by the communication interface ~~command transmission unit~~;~~

the communication interface configured to transmit a second response request command to the data receiving apparatus after receiving the first response message from said data receiving apparatus, the second response request command including third authentication data generated based on the shared data, and receive a second response message to the second response request command from the data receiving apparatus, said second response message containing fourth authentication data generated at the data receiving apparatus based on the shared data and a second sequence number included in the second response request command indicating a position of the second response request

command in the sequence of response request command to be transmitted by the command transmission unit; and

an authentication unit configured to produce an authentication result for said data receiving apparatus based on the fourth authentication data included in the second response message ~~expected authentication value generated by said expected value generation unit and said authentication data in the response message;~~

a measurement unit configured to measure a response time between transmitting the second response request command and receiving the second response message; and

a judgment unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time.

2. (Currently Amended) The data transmitting apparatus recited in claim 1, wherein:

~~said command transmission unit is further configured to transmit said response request command a maximum of N times, wherein N is an integer value;~~

~~said control unit is further configured to receive the response messages from the data receiving apparatus for each of the N transmitted response request commands; and~~

said authentication unit is further configured to produce authentication results based on said second authentication data in said first ~~each received~~ response message;

said measurement unit is configured to measure a response time between transmitting the first response request command and receiving said first response message; and

said judgment unit is configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time.

3. (Currently Amended) A data transmission method comprising:

generating, at a data transmitting apparatus, first authentication data based on shared data shared with a data receiving apparatus;

transmitting a first response request command to [[a]] said data receiving apparatus, said first response request command including said first authentication data;

receiving a first response message to the first response request command from the data receiving apparatus at [[a]] said data transmitting apparatus, the response message including second authentication data, which is generated in the data receiving apparatus prior to the data receiving apparatus receiving the response request command, the authentication data being based on the shared data shared among the data transmitting apparatus and said data receiving apparatus; generating an expected authentication value based on the shared data and a first sequence number included in the first response request command indicating, the sequence number indicating an ordinal a position of the first response request command in a sequence of response request commands to be transmitted to the data transmitting receiving apparatus;

transmitting a second response request command from the data transmitting apparatus to the data receiving apparatus after receiving the first response message from said data receiving apparatus, the second response request command including third authentication data generated based on the shared data;

receiving, at the data transmitting apparatus, a second response message to the second response request command from the data receiving apparatus, said second response message containing fourth authentication data generated at the data receiving apparatus based on the shared data and a second sequence number included in the second response request command indicating a position of the second response request command in the sequence of response request command to be transmitted by the data transmitting apparatus;

producing an authentication result for said data receiving apparatus based on ~~the expected authentication value and~~ said fourth authentication data included in the second response message;

measuring a response time between transmitting the second response request command and receiving the second response message; and

judging if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time.

4. (Currently Amended) A non-transitory computer program storage medium storing computer program instructions which when executed by a data transmitting apparatus ~~computer~~ cause the data transmitting apparatus ~~computer~~ to perform the following method steps:

generating first authentication data based on shared data shared with a data receiving apparatus;

~~controlling transmission of~~ transmitting a first response request command to a data receiving apparatus, said first response request command including said first authentication data;

~~controlling reception of~~ receiving a first response message to the first response request command from the data receiving apparatus, the response message including second authentication data, ~~which is generated [[in]]~~ at the data receiving apparatus prior to the data receiving apparatus receiving the command, the authentication data being based on the shared data ~~shared among the computer and said data receiving apparatus;~~

~~controlling generation of an expected authentication value based on the shared data~~ and a first sequence number included in the first response request command indicating, the ~~sequence number indicating an ordinal~~ a position of the first response request command in a

sequence of response request commands to be transmitted to the data transmitting ~~receiving~~ apparatus;

transmitting a second response request command to the data receiving apparatus after receiving the first response message from said data receiving apparatus, the second response request command including third authentication data generated based on the shared data;

receiving a second response message to the second response request command from the data receiving apparatus, said second response message containing fourth authentication data generated at the data receiving apparatus based on the shared data and a second sequence number included in the second response request command indicating a position of the second response request command in the sequence of response request command to be transmitted by the data transmitting apparatus;

~~controlling production of~~ producing an authentication result for said data receiving apparatus based on ~~the expected authentication value and~~ said fourth authentication data included in the second response message;

~~controlling measurement of~~ measuring a response time between transmitting the second response request command and receiving the second response message; and

judging if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time.

5. (Canceled)

6. (Currently Amended) A data receiving apparatus configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and a response time between sending a response request command and receiving a response message, the data receiving apparatus comprising:

a communication interface ~~command receiving unit~~ configured to receive [[the]] a first response request command from the data transmitting apparatus, the first response request command including first authentication data generated at the data transmitting apparatus based on shared data shared with the data receiving apparatus;

~~an authentication data generation unit~~ a processor configured to generate a first response message to the first response request command, the first response message including second ~~said~~ authentication data generated by the processor based on ~~said~~ shared data and a first sequence number included in the first response request command indicating a position of the first response request command in a sequence of response request commands to be transmitted to the data receiving apparatus from the data transmitting apparatus ~~shared with the data transmitting apparatus by subjecting said shared data to a predetermined process before said response request command is received from said data transmitting apparatus;~~

~~a response message generation unit configured to generate the response message to said response request command before said response request command is received from said data transmitting apparatus, said response message including said authentication data; and~~

~~a transmission unit~~ the communication interface configured to transmit said first response message to said data transmitting apparatus ~~when~~ in response to said first response request command [[is]] received from said data transmitting apparatus;

the communication interface configured to receive a second response request command from the data transmitting apparatus, the second response request command including third authentication data generated at the data transmitting apparatus based on the shared data;

the processor configured to generate a second response message to the second response request command, the second response message including fourth authentication data generated by the processor based on said shared data and a second sequence number included

in the second response request command indicating a position of the second response request command in the sequence of response request commands to be transmitted to the data receiving apparatus from the data transmitting apparatus; and
the communication interface configured to transmit said second response message to said data transmitting apparatus in response to said second response request command received from said data transmitting apparatus.

7. (Currently Amended) The data receiving apparatus recited in claim 6, wherein:
said shared data is a quasi random number ~~transmitted from said data transmitting apparatus before said response request command is transmitted~~; and
said processor ~~authentication data generation unit~~ is further configured to subject said quasi random number to a Keyed-Hash process to produce a Hash value that is used in [[as] said first and second authentication data.

8. (Currently Amended) The data receiving apparatus recited in claim 6, wherein:
said processor ~~authentication data generation unit~~ is further configured to execute a Keyed-Hash process relative to said quasi random number and information specific to the information processing apparatus to produce a Hash value that is used as said first and second authentication data.

9-12. (Canceled)

13. (Currently Amended) A data reception method for a data receiving apparatus configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and a response time between sending a

response request command and receiving a response message, the data reception method comprising:

receiving ~~[[the]]~~ a first response request command from the data transmitting apparatus, the first response request command including first authentication data generated at the data transmitting apparatus based on shared data shared with the data receiving apparatus;

generating a first response message to the first response request command, the first response message including second ~~said~~ authentication data generated by the processor based on ~~said~~ shared data and a first sequence number included in the first response request command indicating a position of the first response request command in a sequence of response request commands to be transmitted to the data receiving apparatus from the data transmitting apparatus ~~shared with the data transmitting apparatus by subjecting said shared data to a predetermined process before said response request command is received from said data transmitting apparatus;~~

~~generating the response message to said response request command before said response request command is received from said data transmitting apparatus, said response message including said authentication data; and~~

transmitting said first response message to said data transmitting apparatus ~~[[when]]~~ in response to said first response request command ~~[[is]]~~ received from said data transmitting apparatus;

receiving a second response request command from the data transmitting apparatus, the second response request command including third authentication data generated at the data transmitting apparatus based on the shared data;

generating a second response message to the second response request command, the second response message including fourth authentication data generated by the processor based on said shared data and a second sequence number included in the second response

request command indicating a position of the second response request command in the sequence of response request commands to be transmitted to the data receiving apparatus from the data transmitting apparatus; and

transmitting said second response message to said data transmitting apparatus in response to said second response request command received from said data transmitting apparatus.

14. (Currently Amended) A non-transitory computer program storage medium storing computer program instructions which, when executed by a data receiving apparatus computer configured to receive data from a data transmitting apparatus which judges whether data transmission is granted based on authentication data and a response time between sending a response request command and receiving a response message, causes the data receiving apparatus computer to perform the following method steps:

receiving a first response request command from the data transmitting apparatus, the first response request command including first authentication data generated at the data transmitting apparatus based on shared data shared with the data receiving apparatus;

generating a first response message to the first response request command, the first response message including second authentication data generated by the processor based on said shared data and a first sequence number included in the first response request command indicating a position of the first response request command in a sequence of response request commands to be transmitted to the data receiving apparatus from the data transmitting apparatus;

transmitting said first response message to said data transmitting apparatus in response to said first response request command received from said data transmitting apparatus;

receiving a second response request command from the data transmitting apparatus,
the second response request command including third authentication data generated at the
data transmitting apparatus based on the shared data;

generating a second response message to the second response request command, the
second response message including fourth authentication data generated by the processor
based on said shared data and a second sequence number included in the second response
request command indicating a position of the second response request command in the
sequence of response request commands to be transmitted to the data receiving apparatus
from the data transmitting apparatus; and

transmitting said second response message to said data transmitting apparatus in
response to said second response request command received from said data transmitting
apparatus

~~controlling the reception of the response request command from the data transmitting~~
~~apparatus;~~

~~controlling generation of said authentication data based on shared data shared with the~~
~~data transmitting apparatus by subjecting said shared data to a predetermined process before~~
~~said response request command is received from said data transmitting apparatus;~~

~~controlling generation of the response message to said response request command~~
~~before said response request command is received from said data transmitting apparatus, said~~
~~response message including said authentication data; and~~

~~controlling transmission of said response message to said data transmitting apparatus~~
~~when said response request command is received from said data transmitting apparatus.~~

15-26. (Canceled)